

## **A Lucas based cryptosystem analog to the ElGamal cryptosystem and elliptic curve cryptosystem**

### **ABSTRACT**

In this paper, a new cryptosystem will be developed which is analogue to ElGamal encryption scheme and based on Lucas sequence in the elliptic curve group over finite field. In this encryption scheme, an Elliptic curve Diffie-Hellman (ECDH) key agreement be the first part of the encryption, the keys of this encryption scheme is defined based on elliptic curve and the order of the group  $G$ . The Lucas sequence will be used for the computations of plaintext and ciphertext in the process of encryption and decryption respectively.

**Keyword:** Decryption; Elliptic curve; Encryption; Lucas sequence